CLAIMS

What is claimed is:

1. A method of preventing an attack on a network, wherein the attack comprises injecting a spurious transmission control protocol (TCP) segment into a TCP connection between a sender and a receiver, the method comprising the computer-implemented steps of:

receiving a duplicate TCP ACK message;

incrementing a false duplicate ACK counter when a TCP re-transmission buffer maintained by the receiver is empty;

when the false duplicate ACK counter is equal to a specified strike factor, sending a corrective ACK message that provides a correct sequence value and ACK value.

2. A method as recited in Claim 1, wherein the specified strike factor is a value in a range of 1 to 10.

3. A method as recited in Claim 1, wherein the steps are performed by an endpoint node acting as the receiver of data in the TCP connection.

4. A method as recited in Claim 1, wherein the steps are performed by a TCP application of an operating system of a network infrastructure element.

5. A method as recited in Claim 1, wherein the steps are performed by a TCP process, stack, adapter or agent hosted by or associated with an operating system of a personal computer, workstation or other network end station.

6. A method as recited in Claim 1, further comprising the steps of:

receiving the corrective ACK message;

determining whether the correct sequence value is less than another sequence value of a segment in a re-assembly buffer;

discarding the segment from the re-assembly buffer when the correct sequence value is less than the other sequence value of a segment in the re-assembly buffer.

7. A method as recited in Claim 6, wherein the discarding step comprises discarding all segments in the re-assembly buffer.

8. A method of preventing an attack on a network, wherein the attack comprises injecting a spurious transmission control protocol (TCP) segment into a TCP connection between a sender and a receiver, the method comprising the computer-implemented steps of:

receiving a particular TCP segment;

determining a sequence value gap as between the particular TCP segment and a prior TCP segment previously placed in a re-assembly buffer maintained by the receiver;

determining whether the sequence value gap is too large according to a specified heuristic;

if the sequence value gap is too large, then performing the steps of:

creating and sending a dummy segment carrying a particular sequence value that is just prior to a last properly acknowledged sequence value;

receiving an acknowledgment of the dummy segment;

determining whether a second sequence value carried in the acknowledgment is less than a third sequence value of the first TCP segment; and

discarding the particular TCP segment from the re-assembly buffer when the second sequence value carried in the acknowledgment is less than the third sequence value of the particular TCP segment.

9. A method as recited in Claim 8, wherein the specified heuristic holds when a re-assembly gap value is greater than one-half of a then-current window size.

10. A method as recited in Claim 8, wherein the specified heuristic holds when a re-assembly gap value is greater than the lesser of (a) one-half of a then-current window size or (b) a multiple of a maximum allowed segment size.

11. A method as recited in Claim 8, wherein the specified heuristic holds when a query threshold is greater than a function of then-current bandwidth and then-current delay.

12. A method as recited in Claim 8, wherein the specified heuristic holds when a query threshold is greater than a function of a round-trip time (RTT) estimate, a then-current available bandwidth value, and window size.

13. A method as recited in Claim 8, wherein the specified heuristic holds when a query threshold value is less than or equal to a re-assembly gap value and the re-assembly gap value is less than or equal to a receive window value.

14. A method as recited in Claim 13, wherein the re-assembly gap value comprises a sequence value of a first segment in the re-assembly buffer less a next expected segment value.

15. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) segment with a spurious or unwanted DATA segment, comprising means for performing any of the steps of Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, or 14.

16. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) segment with spurious or unwanted DATA segment, comprising:

a processor;

one or more stored sequences of instructions that are accessible to the processor and which, when executed by the processor, cause the processor to carry out the steps of any of Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, or 14.

17. A computer-readable medium carrying one or more sequences of instructions for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) segment with unwanted or spurious DATA , wherein the execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of any of Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, or 14.